AMENDMENTS TO THE CLAIMS

Listing of Claims:

1. (Currently Amended) A computer product, comprising:

first computer readable program code embodied in a computer usable medium to cause a computer to receive a message that includes an encrypted hardware configuration code for configuring hardware and receive a key associated with an encrypted code defining a unique hardware configuration;

second computer readable program code embodied in a computer usable medium to cause a computer to decrypt the encrypted code based upon the stored key;

third computer readable program code embodied in a computer usable medium to cause a computer to program a legic arrayre-configurable hardware block based upon the decrypted key to establish a unique hardware configuration, wherein the configuration is changed at regular intervals; and

fourth computer readable program code embodied in a computer usable medium to cause a computer to perform a decryption operation on encrypted information utilizing the unique hardware configuration.

- (Original) The computer product claimed in claim 1, further comprising:
 fifth computer readable program code embodied in a computer usable medium to cause
 a computer to route encrypted information through a peripheral device to the logic array.
- 3. (Original) The computer product claimed in claim 1, further comprising: fifth computer readable program code embodied in a computer usable medium to cause a computer to route the incoming information through a memory interface to the logic array.
- 4. (Original) The computer product claimed in claim 1, wherein the logic array includes a programmable an array of gates.
 - 5. (Currently Amended) An electronic system comprising: at least one peripheral device;
 - a memory for storing a key associated with incoming information; and
- a chipset in communication with the at least one peripheral device, the chipset including circuitry to receive a message that includes an encrypted hardware configuration code for configuring hardware, program an array of gates a re-configurable hardware block based upon the key associated with the incoming information to establish a unique hardware configuration, wherein the configuration is changed at regular intervals, and decrypt the incoming information

based on the programmed array of gates and circuitry to perform a decryption operation on the incoming information based on the configured array of gates.

- 6. (Original) The electronic system claimed in claim 5, further comprising: circuitry for routing the incoming information from a peripheral device through the configured array of gates.
- 7. (Original) The electronic system claimed in claim 5, further comprising: circuitry for routing the incoming information from a memory device through the configured array of gates.
- 8. (Original) The electronic system claimed in claim 5, wherein the memory is a non-volatile memory.
- 9. (Original) The electronic system claimed in claim 5, wherein the key is a public key.
- 10. (Previously Presented) The electronic system claimed in claim 5, wherein the key is a non-public key.
- 11. (Currently Amended) A method for decrypting encrypted information, comprising:

receiving a message that includes an encrypted hardware configuration code for configuring hardware;

storing a key associated with the encrypted code defining a unique hardware configuration;

decrypting the encrypted code based upon the stored key;

establishing a unique hardware configuration based upon the encrypted code, wherein the configuration is changed at regular intervals; and

performing a decryption operation on encrypted information utilizing the unique hardware configuration.

- 12. (Original) The method claimed in claim 11, further comprising: routing encrypted information through a peripheral device to the logic array.
- 13. (Original) The method claimed in claim 11, further comprising: routing the incoming information through a memory interface to the logic array.

042390.P9941 3 109/753,246

- 14. (Previously Presented) The method claimed in claim 11, wherein the logic array includes a programmable an array of gates.
- 15. (Currently Amended) A method for decrypting encrypted information, comprising:

initiating a programmable array of gates;

receiving a message that includes an encrypted hardware configuration code for configuring hardware;

decrypting the code using a key;

command.

programming the programmable array of gates to provide a unique hardware configuration, wherein the configuration is changed at regular intervals; and decrypting the information utilizing the unique hardware configuration.

- 16. (Original) The method claim in claim 15, further comprising: routing the incoming information through a peripheral device to the configured array of gates.
- 17. (Original) The method claimed in claim 15, further comprising: routing the incoming information through a memory interface to the configured array of gates.
- 18. (Original) The method claimed in claim 15, wherein programming an array of gates based upon the key associated with the incoming information further comprises: programming the array of gates to provide for a unique hardware configuration upon
- 19. (Original) The method claimed in claim 15, wherein programming an array of gates based upon the key associated with the incoming information further comprises: receiving instructions from a processor.
- 20. (Original) The method claimed in claim 15, further comprising storing the key in non-volatile memory.